REMARKS

Figure 1 has been amended to illustrate that server 112 includes a CPU 150, operating system 152, memory 154 and hard drive storage 156. The specification has likewise been amended to state that server 112 includes a known CPU 150, operating system 152, memory 154 and hard drive storage 156. Support is found in the term "server" 112 which was included in the original drawings and specification (Figure 1 and Page 5 lines 2-5) and is well understood to include a CPU, operating system, memory and hard disk storage. Moreover, the original specification describes the message transfer agent, spam detector program, ranger finder program and monitor program all as programs residing and operating (executing) in server 112 (Page 5 line 1, Page 5 lines 20-21, Page 8 lines 5-6 and Page 9 lines 11-13, and Page 6 lines 6-8) and this requires a CPU, operating sytem, memory and hard disk storage. "Figures 2(A) and 2(B) form a flow chart illustrating operation of the spam filter program 119, spam detector 121, optional spam detector 123, ranger finder progam 130 and monitor program 132 in accordance with the present invention." Page 6 lines 6-8. No new matter has been added.

The specification has also been amended to recite that the message transfer agent, spam detector program, ranger finder program and monitor program may reside in storage 156. Support is found on Page 5 line 1, Page 5 lines 20-21, Page 8 lines 5-6 and Page 9 lines 11-13, and Page 6 lines 6-8 which state that these programs may reside and operate (execute) in server 112, and it is well known that programs are stored/installed on a hard drive storage awaiting operation/execution. No new matter has been added.

Claims 7 and 15 were found objectionable because of a missing word "e-mail" at the end of these claims, and this error has been corrected above.

Claims 17-20 have been canceled without prejudice, in lieu of new claims 21-28.

Claims 1-20 were rejected under 35 USC 103 based on Kirsch (US Patent Application 2004/0177120) in combination with Spamhaus. Applicants respectfully traverse this rejection based on the following.

Kirsch (US Patent Application 2004/0177120) teaches the following process for blocking spam.

> "The true sender of an e-mail message [is identified] based on data in the e-mail message and then assessing the reputation, or rating, of the true sender to determine whether to pass the e-mail message on to the recipient. The true sender may be identified in one embodiment by combining the full or base e-mail address and the IP address of the network device used to hand off the message to the recipient's trusted infrastructure (i.e. the sender's SMTP server, which sends the e-mail to the recipient's mail server or a forwarding server used by the recipient); this IP address is used because it is almost impossible to forge. In other embodiments, different pieces of information can be combined. In yet another embodiment, a digital signature in the e-mail message may be used to identify the true sender. Other embodiments may combine the digital signature with other data (the full or base e-mail address, the final IP address, the domain name associated with the final IP address) in the e-mail message. Once the true sender has been identified, the reputation of the true sender is assessed in order to determine whether the e-mail should be passed to the recipient or disposed of according to the recipient's preferences for handling suspect junk e-mail. A central database tracks statistics about true senders which are supplied by any user of the e-mail network. These statistics include the number of user who have placed the true sender on a whitelist, the number of users who have placed the true sender on a black list, the number of e-mail's the true sender has sent since any user in the e-mail network first received a message from the true sender, etc. Based on the information stored at the central database, the reputation of a true sender is evaluated to determine whether it is above a threshold set by the recipient. If the true sender's reputation does exceed the threshold, the message is passed to the recipient. Otherwise, the message is disposed of according to the recipient's preferences." Kirsch (US Patent Application 2004/0177120) Paragraphs [0011-0013].

Amended claim 1 recites a method of blocking unwanted e-mails. An e-mail is determined to be unwanted. A source IP address of the unwanted e-mail is determined. A registrant of the source IP address of the unwanted e-mail is determined, and an entity that manages registration of IP addresses is queried to determine other source IP addresses registered to the registrant of the source IP address of the unwanted e-mail. In response, subsequent e-mails from the other IP addresses are blocked.

In contrast to amended claim 1, Kirsch (US Patent Application 2004/0177120) does not teach that a registrant of the source IP address of the unwanted e-mail is determined, and an entity that manages registration of IP addresses is queried to determine other source IP addresses registered to the registrant of the source IP address of the unwanted e-mail, and in response, subsequent e-mails from the other IP addresses are blocked. Rather, Kirsch (US Patent Application 2004/0177120) discloses that the true sender of an e-mail message is identified based on data in the e-mail message and then the reputation, or rating, of the true sender is assessed to determine whether to pass the e-mail message on to the recipient. The Examiner acknowleges the broad deficiency of Kirsch (US Patent Application 2004/0177120), "Kirsch does not expressly disclose determining other source IP addresses owned or registerd by an owner or registrant of the source IP address of said unwanted e-mail." Spamhaus (web.archive.org/web/20011211165) (which the Examiner asserts was published in 2001) discloses:

> "The Spamhaus Block List ("SBL") is a list of IP addresses compiled by the same team that maintains the ROKSO database, broadcast in realtime to independent DNS-based "Blocklist" systems. All IPs on the SBL belong to known spammers, spam gangs, or spam support services. The SBL includes IPs from both the ROKSO database and IPs of spam services listed in the Spamhaus database. All SBL entries are backed up with evidence which has fully satisfied the Spamhaus Project team that the IP is under the control of a spam outfit or a spam-haven and that the IP or netblock represents an unwanted nuissance or threat to users of the SBL. All IPs on the SBL can be quieried to see the reason for

inclusion of each. Major SBL entries (entries greater than single /32s) are listed here together with the reason for listing."

In the beginning of the foregoing excerpt from Spamhaus, Spamhaus states that individual IP addresses of spammers are identified and put in a list, but there is no teaching of the feature of amended claim 1 where a registrant of the source IP address of the unwanted e-mail is determined, and an entity that manages registration of IP addresses is queried to determine other source IP addresses registered to the registrant of the source IP address of the unwanted e-mail, and in response, subsequent e-mails from the other IP addresses are blocked.

In the latter part of the foregoing excerpt from Spamhaus, Spamhaus discloses that all SBL entries are backed up with evidence which has fully satisified the Spamhaus Project team that the IP is under the control of a spam outfit or a spam-haven and that the IP or **netblock** represents an unwanted nuissance of threat to users of the SBL. The term "netblock" is not well defined in Spamhaus. In contrast to amended claim 1, Spamhaus does not teach how the netblock is determined. If the term "netblock" means a range of IP addresses, it is possible that Spamhaus determines the netblock from the bounds of a cluster of IP addresses associated with multiple detected spam, and inferences as to logical end points. Also, in contrast to amended claim 1, Spamhaus does not teach that the IP addresses of the netblock are registered to the registrant of the source IP address of the unwanted e-mail. It is possible that the IP addresses of the netblock are registered to an intermediary mail server or ISP. Therefore, Spamhaus does not fill the gap of Kirsch (US Patent Application 2004/0177120) for at least two reasons.

In response to the Office Action, Applicants also searched the current web site of Spamhaus, and identified "SBL Policy & Listing Criteria" at http:/www.spamhaus.org/sbl/policy.html, which is enclosed and states "SBL listings are backed up with evidence which has fully satisifed the SBL team that the IP addresses or IP range is under the control of a spammer, spam operation or a spam support service and represents unwanted nuissance or threat to mail systems using the SBL." However, this "SBL Policy & Listing Criteria" is not dated, and the original publication date of this "SBL Policy & Listing Criteria" is

unknown to Applicants. Moreover, even if "SBL Policy & Listing Criteria" is prior art relative to the present patent application, "SBL Policy & Listing Criteria" has the same deficiencies as the archived Spamhaus document cited by the Examiner. In contrast to amended claim 1, "SBL Policy & Listing Criteria" does not teach how the IP range is determined. It is possible that "SBL Policy & Listing Criteria" determine the IP range from the bounds of a cluster of IP addresses associated with multiple detected spam, and inferences as to logical end points. Also, in contrast to amended claim 1, "SBL Policy & Listing Criteria" does not teach that the IP addresses of the netblock are registered to the registrant of the source IP address of the unwanted e-mail. It is possible that the IP addresses of the netblock are registered to an intermediary mail server or ISP. Therefore, "SBL Policy & Listing Criteria" does not fill the gap of Kirsch (US Patent Application 2004/0177120) for at least two reasons, even if "SBL Policy & Listing Criteria" is prior art.

Claims 2-8 depend on amended claim 1 and therefore, distinguish over the prior art for the same reasons that amended claim 1 distinguishes thereover.

Independent, amended claim 9 distinguishes over the prior art for the same reasons that independent claim 1 distinguishes over the prior art. In addition claim 9 recites an automated/computer-programmed technique for blocking unwanted e-mails. Claims 10-16 depend on amended claim 9 and therefore, distinguish over the prior art for the same reasons that amended claim 9 distinghishes thereover.

Independent, new claim 21 distinguishes over the prior art for the same reasons that independent claim 1 distinguishes over the prior art. In addition claim 21 recites an automated/computer-programmed technique for blocking unwanted e-mails. Claims 22-28 depend on claim 21 and therefore, distinguish over the prior art for the same reasons that new claim 21 distinghishes thereover.

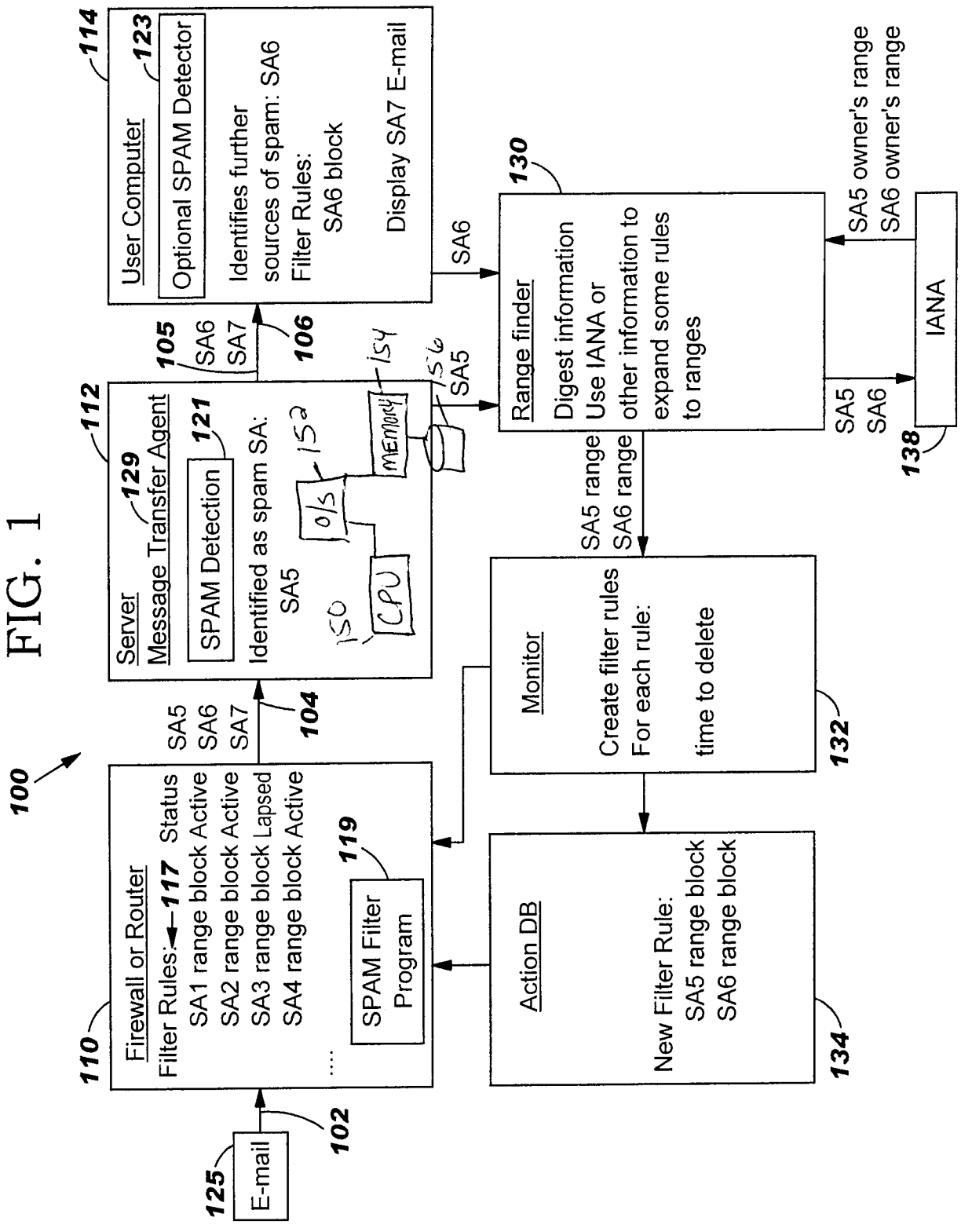
Based on the foregoing, Applicants request allowance of the present patent application as amended above.

Respectfully submitted,

Dated: 07/31/08
Phone: 607-429-4368
Fax: 607-429-4119

/Arthur J. Samodovitz/
Arthur J. Samodovitz
Reg. No 31,297

FIG. 1


100
E-mail
125
102
Firewall or Router
110
Filter Rules:
117
Status
SA1 range block Active
SA2 range block Active
SA3 range block Lapsed
SA4 range block Active
....
SPAM Filter Program
119
SA5
SA6
SA7
104
Server
Message Transfer Agent
129
SPAM Detection
121
Identified as spam SA:
SA5
CPU
150
O/S
152
Memory
154
156
SA5
105
SA6
SA7
106
User Computer
114
Optional SPAM Detector
123
Identifies further sources of spam: SA6
Filter Rules:
SA6 block
Display SA7 E-mail
SA6
Range finder
130
Digest information
Use IANA or other information to expand some rules to ranges
SA5 range
SA6 range
SA5 owner's range
SA6 owner's range
SA5
SA6
IANA
138
Monitor
Create filter rules
For each rule:
time to delete
132
Action DB
New Filter Rule:
SA5 range block
SA6 range block
134